



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,168	07/03/2001	John I. Okimoto	018926-006800US	9604
20350	7590	01/12/2005	EXAMINER	
TOWNSEND AND TOWNSEND AND CREW, LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834			ZAND, KAMBIZ	
		ART UNIT	PAPER NUMBER	
		2132		

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/898,168	OKIMOTO ET AL.
	Examiner Kambiz Zand	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 03 July 2001.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-24 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-24 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 03 July 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date 06&10 of 2003.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____.

DETAILED ACTION

1. **Claims 1-24** have been examined.

Information Disclosure Statement PTO-1449

2. The Information Disclosure Statement submitted by applicant on 06/09/2003 and 10/10/2003 have been considered. Please see attached PTO-1449.

Specification

3. The disclosure is objected to because of the following informalities: Please update cross-references to related applications information (page 1, lines 5-27 of the specification).

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention

was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over in Candelore (6,363,149 B1) in view of Hoffman et al (5,613,012 A).

As per claims 1, 3, 4, 7, 8, 10-14, 17 and 24 Candelore (6,363,149 B1) teach in a cable system, an encryption renewal system for generating one or more entitlement control messages, the messages containing cryptographic keys for allowing a subscriber set-top box to decrypt content encrypted off-line, the entitlement control message being forwarded with the content to the subscriber terminal, the encryption renewal system comprising: a first computing platform for receiving a request to generate the entitlement control messages, the first computing platform performing non-secure tasks associated with the entitlement control messages; a second computing for generating the entitlement control messages, the second computing platform performing secure tasks associated with the entitlement control messages; and the first computing platform forwarding the entitlement control messages to enable the subscriber set-top box to de-crypt the pre-encrypted content (see abstract; fig.1-3 and associated text; col.10, lines 33-67; col.11 and col.12, lines 1-14); transmitting one or more keys from the first platform to a subscriber as recited in claim 3, 13 and 17 and all limitation set forth in the claims (see fig.1-7b and associated text) and but do not explicitly disclose physical separation of the first platform with the second platform; and one or more firewalls between the first, second or third computing platforms for enhancing security of the encryption renewal system. However Hoffman et al (5,613,012 A) disclose physical

separation of the first platform with the second platform or third; and one or more firewalls between the first and the second computing platforms for enhancing security of the encryption renewal system (see fig.1 and associated text; col.14, lines 20-27; col.18, lines 6-53; col.24, lines 65-67; col.25, lines 1-8). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hoffman's firewall security system between two physically located platform in a network environment in order to protect the system from electronic eavesdropping and electronic intrusion and viruses during content transmission or distribution.

As per claim 2 Candelore (6,363,149 B1) teach the system of claim 1 wherein the second computing platform further comprises an application specific integrated circuit chip for generating the entitlement control messages (see col.6, lines 21-51; fig.2).

As per claims 5, 18 Candelore (6,363,149 B1) teach the system of claim 3 further comprising a database for storing the keys to be included in the control messages (see col.6, lines 43-46; col.10, lines 22-24).

As per claim 6 Candelore (6,363,149 B1) teach the system of claim 3 wherein the key is a group or periodical key from a conditional access system for controlling a population of set-top boxes (see col.10, lines 43-67).

As per claim 9 Candelore (6,363,149 B1) teach all limitation of the system of claim 3

but do not explicitly disclose a web server accepting requests from the first computing platform to generate the control messages. However Hoffman (5,613,012 A) disclose a web server accepting requests from the first computing platform to generate the control messages (see fig.1 and associated text). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hoffman's firewall security system between two physically located platform in a network environment using a web server in order to protect the system from electronic eavesdropping and electronic intrusion and viruses during content transmission or distribution.

As per claim 15 Candelore (6,363,149 B1) teach the system of claim 14 wherein the application specific integrated circuit re-encrypts the one or more cryptographic keys for external storage (as applied to claim 1 and 5 above).

As per claim 16 Candelore (6,363,149 B1) teach the system of claim 13 wherein the means for storing stores information about which video on demand system associated with the conditional access system (see fig.9A-D and 7B).

As per claim 19 Candelore (6,363,149 B1) teach the method of claim 17 wherein the data contains both cryptographic keys and one or more operating parameters for the off-line encryption device (see col.7, lines 36-47).

As per claim 20 Candelore (6,363,149 B1) teach the method of claim 19 wherein the

operating parameter is a maximum number of encryption sessions allocated to the off-line encryption device (see col.7, lines 36-47 as applied to claim 17).

As per claim 21 Candelore (6,363,149 B1) teach the method of claim 17 where the step of generating further comprises determining the operating parameters of the off-line encryption device (see col.7, lines 36-47 and as applied to claim 17).

As per claim 22 Candelore (6,363,149 B1) teach the method of claim 18 wherein the storing one or more cryptographic keys further comprises, storing the one or more cryptographic keys in the off-line encryption device; and storing the one or more cryptographic keys in the encryption renewal system (see col.7, lines 36-47 and as applied to claim 17).

As per claim 23 Candelore (6,363,149 B1) teach the method of claim 19 further wherein the one or more cryptographic keys include any one or more of a secret shared key, a private key, and a public key (see col.10, lines 30-34).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S. Patent No. US (5,627,982A) teach data security scheme for point-to-point communication session.

U.S. Patent No. US (6,771,657 B1) teach non real-time delivery of MPEG-2 programs via an MPEG-2 transport stream.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Kambiz Zand

01/06/05
AV 2132